REMARKS

This Amendment is filed in response to the FINAL Office Action mailed January 5, 2010. A Request for Continued Examination and the associated fee is also filed herewith. All objections and rejections are respectfully traversed.

Claims 1-5 and 30-67 are in the case.

No new claims have been added.

Claims 1 and 30 have been amended.

Interview Summary

Applicant would like to thank Examiner Colan and primary Examiner Corrielus for conducting the Applicant Initiated Interview on February 25, 2010 and for helping to advance this Application closer to allowance. Generally, as will be elaborated upon in greater detail below, the issue discussed involved Applicant's use of **sending a NFS file handle** ***with encryption key metadata inserted in the NFS file handle to a client***. Specifically, Applicant discussed how the primary prior art reference (i.e., Chandrashekhar) strips off metadata before sending a requested file to a client. As such, Examiner cited the secondary prior art reference (i.e., Ryuutou) to show sending the (encryption key) metadata to a client. However, Applicant noted that Ryuutou's metadata sent back to the client was a session ID. Examiner Corrielus agreed with Applicant that the session ID of the Ryuutou reference was not encryption key metadata. As such, Applicant noted that (1) if Chandrashekhar strips off metadata (e.g., encryption key metadata or otherwise) before sending a requested file to a client, and (2) if the metadata that is sent by Ryuutou back to the client is not encryption key metadata, then neither reference, taken singly or in any combination, taught or suggested Applicant's claimed novel and non-obvious **sending** ***to a client encryption key metadata inserted in a NFS file handle***.

Examiner Colan then suggested, for the first time on the record, that she did not believe the metadata noted by Chandrashekhar to be stripped off was the encryption key metadata. However, Applicant respectfully noted that if this were true, there would have

been no need to cite Ryuutou to show "sending, by the proxy the file handle with the [encryption key] metadata inserted in the file handle to the client" (see pages 3-4 of the Office Action). Applicant further noted a lack of support in Chandrashekhar for Examiner Colan's suggestion. Finally, Examiner suggested placing claim 30 in claim 1 to put the case in condition for allowance.

While Examiners initially agreed with some aspects of Applicant's discussion, Examiners noted that a closer look at the prior art would be required to verify Applicant's contentions and that another search would be required. Examiners are encouraged to contact the undersigned attorney with any questions. Examiners also noted that if a new search resulted in a new discovery of relevant art, Examiner Colan would contact the undersigned attorney to discuss the art before issuing the next Office Action.

Rejections Under 35 U.S.C. §103

At Paragraph 6 of the Office Action, claims 1-5 and 30-67 were rejected under 35 U.S.C. §103(a) as being obvious over Chandrashekhar et al., U.S. Patent Publication 2005/0033988 published on February 10, 2005 (hereinafter "Chandrashekhar"), and in view of Ryuutou et al., U.S. Patent Application Publication No. 2002/0083191 published on June 27, 2002 (hereinafter "Ryuutou").

Applicant's claimed novel and non-obvious invention, as set out in representative claim 1, comprises in part:

> 1. A method for establishing identity in a file system, comprising:
> receiving, from a client, a first Network File System (NFS) operation concerning an indicated file, the first NFS operation received by a proxy;
> forwarding the first NFS operation from the proxy to be received by a file server;
> returning a NFS file handle associated with the first NFS operation from the file server to the proxy in response to the file server receiving the first NFS operation from the proxy;
> inserting, by the proxy, metadata into the NFS file handle in response to receiving the NFS file handle from the file server, wherein the metadata is an encryption key;

> **sending**, by the proxy in response to receiving the NFS file handle from the file server, **the NFS file handle** ***with the metadata inserted in the NFS file handle to the client*** as a reply to the first NFS operation; and
>
> using, by the client, the metadata and the NFS file handle in a second NFS operation to identify the client and the indicated file.

As an aside, in an interview conducted on August 27, 2009 and in the subsequent Amendment filed on September 8, 2009, Applicant discussed how neither Chandrashekhar nor Ryuutou disclosed an **NFS file handle**. As such, Applicant argued that both Chandrashekhar and Ryuutou failed to teach or suggest Applicant's claimed novel and non-obvious ***inserting encryption key metadata into an NFS file handle*** and then **sending the NFS file handle** ***with the encryption key metadata inserted in the NFS file handle to the client as a reply to the first NFS operation***. Applicant maintains this argument; however, in the interest of advancing prosecution and avoiding the delay in seeking appellate review from the Board of Patent Appeals and Interferences and/or the U.S. Court of Appeals for the Federal Circuit, Applicant respectfully presents an alternative argument. Applicant expressly reserves the right to present these contentions or variations thereof in any appellate procedures.

Chandrashekhar discusses processing file requests sent by a client and received by a proxy using security applications to encrypt, decompress, verify, and decrypt network data by a server receiving the files from the proxy [0058; 0071]. Header policy information is determined, generated, and then stored on the filer server [0055; Fig. 4-5]. However, any metadata added to a file is stripped off before the file is returned to the client [0038].

Ryuutou discloses, in relevant part as cited by Examiner, a client establishing an HTTP connection between the client and a proxy server by initiating a communication connection request [0072-0073]. A session ID is added to header information of an HTTP request [0067; *see also* Fig. 9 below]. Notably, Ryuutou explicitly states that session IDs are identifiers of sessions whose communications have been established [0069; *see also* Fig. 1 below (item **2**: "DETERMINING WHETHER OR NOT

CONNECTION IS ESTABLISHED ACCORDING TO IDENTIFIER WRITTEN IN REQUEST")].

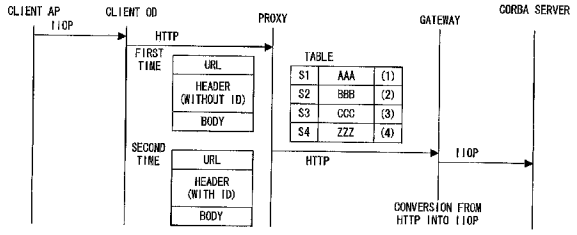

FIG. 9

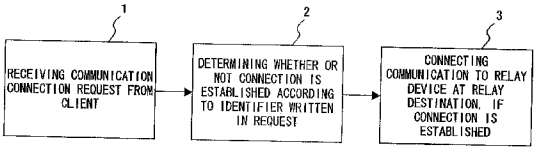

FIG. 1

Applicant respectfully urges that Chandrashekhar, taken singly or in any combination with Ryuutou, does not disclose Applicant's claimed novel and non-obvious use of

sending a NFS file handle ***with encryption key metadata inserted in the NFS file handle to a client***.

Applicant claims, in part, a proxy receiving from a client a first Network File System (NFS) operation concerning an indicated file and forwarding the first NFS operation from the proxy to be received by a file server. Applicant further claims returning a **NFS file handle** associated with the first NFS operation from the file server to the proxy in response to the file server receiving the first NFS operation from the proxy. Applicant further claims inserting, by the proxy, ***encryption key metadata*** into the **NFS file handle**. With that being said, after inserting (the encryption key) metadata into the NFS file handle, Applicant further claims **sending the NFS file handle** ***with encryption key metadata inserted in the NFS file handle to a client***.

Applicant respectfully argues that Chandrashekhar does not teach or suggest Applicant's claimed novel and non-obvious **sending a NFS file handle** ***with encryption key metadata inserted in the NFS file handle to a client***. Specifically, while Chandrashekhar may or may not disclose inserting encryption key metadata into a NFS file handle, Chandrashekhar is explicit in stating that the metadata is stripped off ***before***

the file is returned to the client (see Chandrashekhar at [0038] cited, in relevant part, below):

> …The meta-data is stripped off ***before*** the file data/file attributes are returned to the client… (emphasis added)

Accordingly, not only does Chandrashekhar not teach Applicant's claimed novel and non-obvious **sending a NFS file handle *with encryption key metadata inserted in the NFS file handle to the client***, but Chandrashekhar actually teaches away from doing so. Thus, because Chandrashekhar explicitly teaches away from Applicant's claimed invention, *Chandrashekhar is not an appropriate prior art reference* under 35 U.S.C. §103. Therefore, because Chandrashekhar explicitly teaches away from **sending a NFS file handle *with encryption key metadata inserted in the NFS file handle to the client***, Chandrashekhar fails to teach or suggest Applicant's claimed novel **sending a NFS file handle *with encryption key metadata inserted in the NFS file handle to the client***.

Applicant respectfully argues that Ryuutou does not teach or suggest Applicant's claimed novel and non-obvious **sending a NFS file handle *with encryption key metadata inserted in the NFS file handle to a client***. Specifically, while Ryuutou may or may not teach adding a session ID to header information, Ryuutou explicitly states that a session ID is an identifier of a session between a client and a server whose communications have been started (*see* Ryuutou at [0069] cited, in relevant part, below):

> The already stored session identifiers…are identifiers of sessions whose communications have been started…(emphasis added)

In other words, while Ryuutou may or may not teach adding a session ID to header information, Ryuutou's session ID is not ***encryption key metadata***. Thus, when Ryuutou discloses adding a session ID to header information, Ryuutou is not disclosing adding encryption key metadata to header information. In contrast, Applicant claims sending ***encryption key metadata inserted in the NFS file handle*** to the client. As such, because Ryuutou's definition of a session ID does not include any disclosure or suggestion of

being encryption key metadata, Ryuutou fails to teach or suggest Applicant's claimed novel and non-obvious **sending a NFS file handle** ***with encryption key metadata inserted in the NFS file handle to the client***.

To reiterate:

(I) Even if it is assumed *arguendo* that Chandrashekhar stores encryption key metadata in a NFS file handle, Chandrashekhar does not **send the NFS file handle** ***with encryption key metadata inserted in the NFS file handle to the client***, because Chandrashekhar explicitly states that the metadata is stripped off ***before*** the file is returned to the client. Thus, if encryption key metadata is stored in a NFS file handle, but stripped off before the file handle is returned to the client, then the file handle sent to the client cannot contain encryption key metadata. Therefore, Chandrashekhar fails to teach or suggest Applicant's claimed novel and non-obvious **sending a NFS file handle** ***with encryption key metadata inserted in the NFS file handle to the client***.

(II) Similarly, even if it is assumed *arguendo* that Ryuutou stores a session ID into a NFS file handle, Ryuutou does not **send the NFS file handle** ***with encryption key metadata inserted in the NFS file handle to the client***, because Ryuutou explicitly states that a session ID is an identifier of a session between a client and a server whose communications have been started. Thus, if a session ID is an identifier of a session between a client and a server whose communications have been started, then a session ID cannot be encryption key metadata. This point was conceded by primary Examiner Corrielus during the interview conducted on February 25, 2010. More specifically, if a session ID cannot be encryption key metadata, then sending a NFS file handle with a session ID inserted in the NFS file handle to the client is demonstrably different than **sending a NFS file handle** ***with encryption key metadata inserted in the NFS file handle to the client***. Therefore, Ryuutou fails to teach or suggest Applicant's claimed novel and non-obvious **sending a NFS file handle** ***with encryption key metadata inserted in the NFS file handle to the client***.

Accordingly, Applicant respectfully urges that Chandrashekhar, taken singly or in any combination with Ryuutou, is legally insufficient to render the presently claimed invention obvious under 35 U.S.C. §103. Chandrashekhar and Ryuutou, taken singly or in any combination, fails to teach or suggest Applicant's claimed novel and non-obvious **sending a NFS file handle *with encryption key metadata inserted in the NFS file handle to a client***.

Applicant's Interpretation of the Prior Art

Applicant's interpretation of the prior art references was derived, in part, from the following excerpts:

Chandrashekhar

[0038]…The meta-data relates to key management, length of the original file/dataset, whether the file was compressed prior to encryption or not, integrity checks for file data. The meta-data is stripped off ***before*** the file data/file attributes are returned to the client… (emphasis added)

Ryuutou

[0017] …a communication connection request is received from a client, whether or not a communication connection corresponding to a series of communications is established is determined according to an identifier written in the communication connection request, and the requested communication is connected to a particular relay device as a relay destination of an established communication connection, if the communication connection is established. (emphasis added)

[0057] FIG. 6 is a flowchart showing the process of a communication connection management method in this preferred embodiment. In FIG. 5, when a new communication connection to a gateway is established in correspondence with the initial communication connection request within one session, and a session ID is set, its contents are stored in a memory (table) not shown...(emphasis added)

[0069] The already stored session identifiers and connection numbers are identifiers of sessions whose communications have been started, and numbers of connections established for the sessions respectively. (emphasis added)

[0072] As explained with reference to FIG. 9, the session number S4, and the session ID ZZZ are set by the proxy in correspondence with this communication connection request. The newly set session ID is added to

the header information…and returned…to the client side. (emphasis added)

[0073] At this time, ZZZ as the session ID is added between B and C in the header information shown in FIG. 10. As a method adding a session ID, a method such as Netscape Cookie, with which a browser side can recognize and store, for example, data that is additionally described in an HTTP header, is used. (emphasis added)

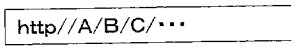

FIG. 10

[0074] A reply including header information to which a session ID is added is returned from a proxy side to a PC side as described above, so that header information including the session ID can be used as the header information in the second and subsequent communication connection requests. (emphasis added)

Conclusion

All new claims and/or claim amendments are believed to be fully supported by Applicant's specification.

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims, and therefore in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

/Michael T. Abramson/

Michael T. Abramson
Reg. No. 60,320
CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210
Telephone: (617) 951-2500
Facsimile: (617) 951-3927